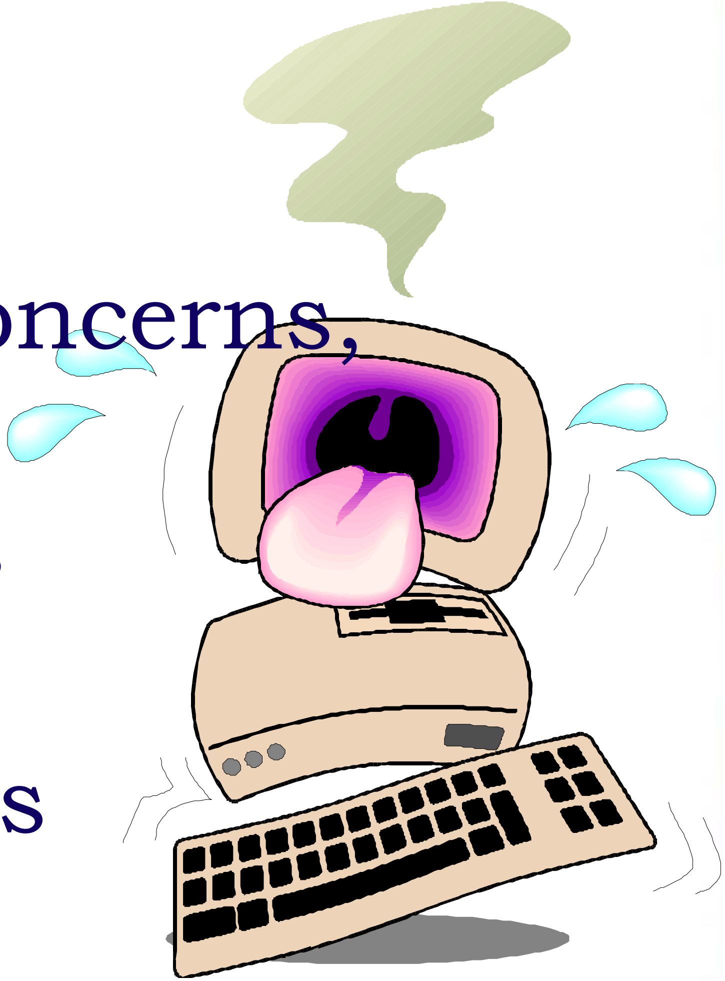
# Critical Infrastructure Assurance

**Iowa Lunch and Learn Program**
**November 27th, 2001**

**Kip Peters**
**Chief Information Security Officer**
**State of Iowa**
**515-725-0362**
**Kip.Peters@itd.state.ia.us**
**http://www.itd.state.ia.us/security/**

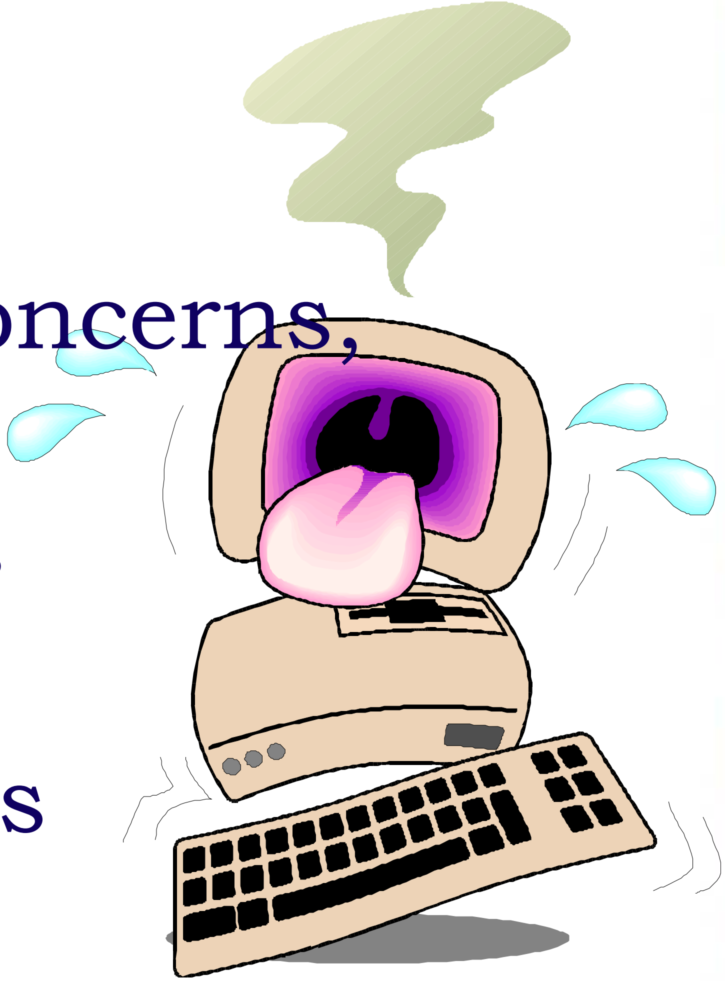
# Overview

- Introduction
- Concepts, Concerns, Impacts
- Case Studies
- Issues
- Contributions
- Conclusion



# Overview

- *Introduction*
- Concepts, Concerns, Impacts
- Case Studies
- Issues
- Contributions
- Conclusion



# Cyber Terrorism Defined

*The purposeful or threatened use of politically, socially, economically, or religiously motivated cyber warfare or cyber-targeted violence, conducted by a non-state or state-sponsored group for the purposes of creating fear, anxiety, and panic in the target population, and disruption of military and civilian assets.*

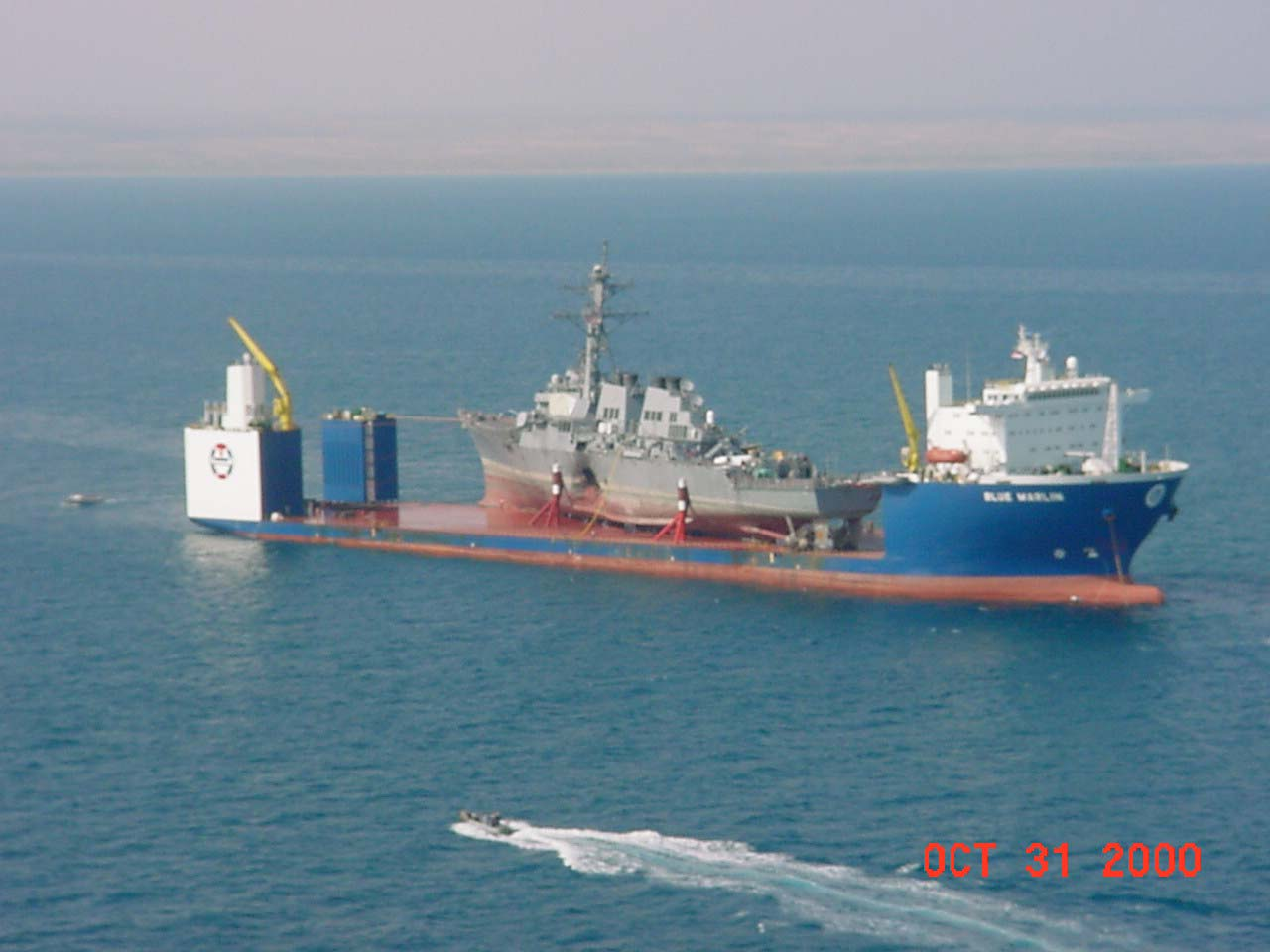
- James K. Campbell

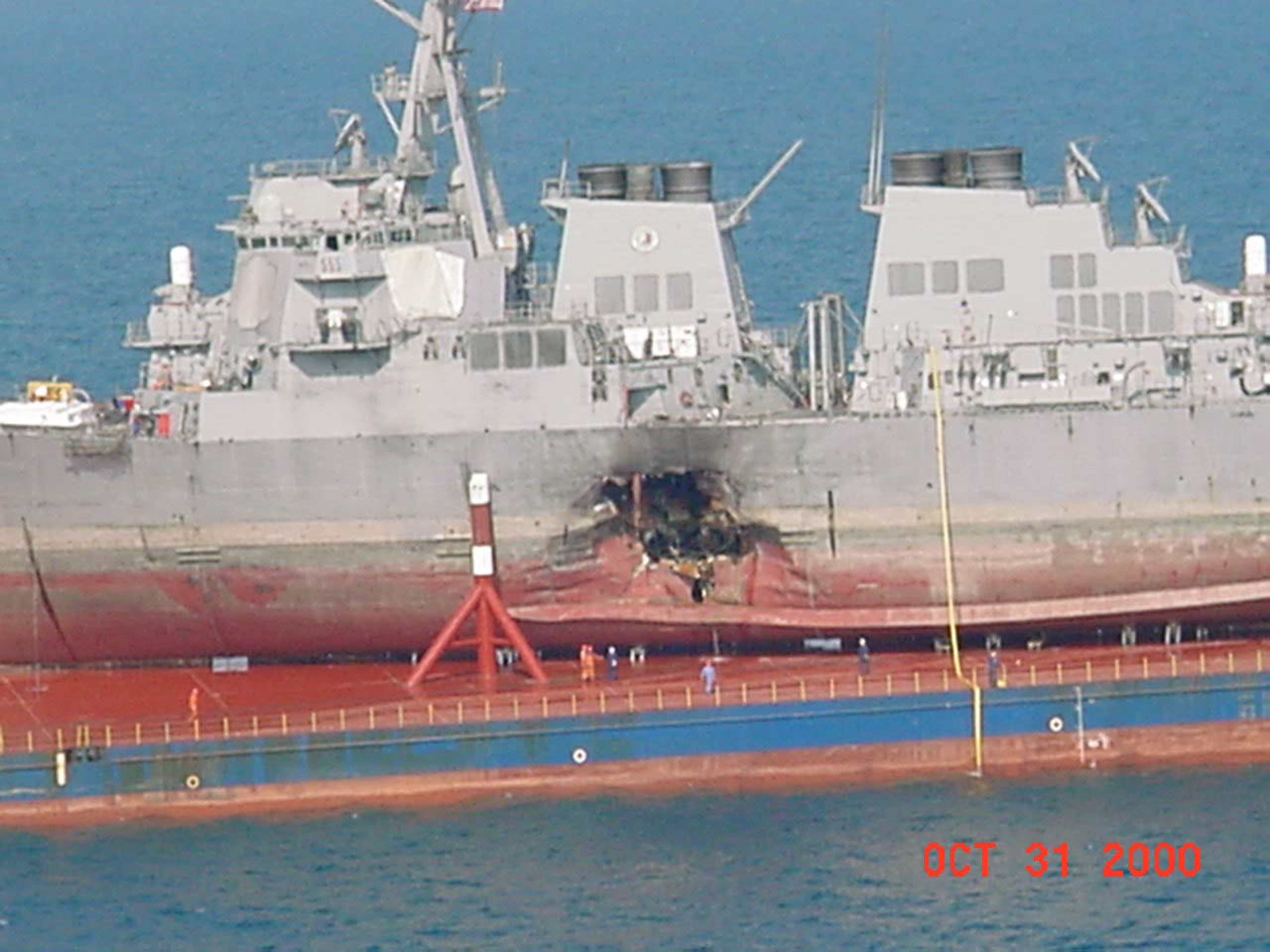
# Cyber Terrorism

- Defined by the target, not the means
- Any attack on an information function for the purpose of creating fear, anxiety, and/or panic in the target population
- Not the run of the mill hacker

# Cyber Terrorism

- Real danger from extremist groups with a single focus or cause
- Willing to go the extra yard(s)
- Serious bodily harm
- Serious property damage


BLUE MARLIN
OCT 31 2000



OCT 31 2000

# Cyber Terrorism

"Today's lurid speculations turn into tomorrow's headlines, making it hard to dismiss even the most far-fetched scenarios."

--Brian Michael Jenkins
RAND Corporation

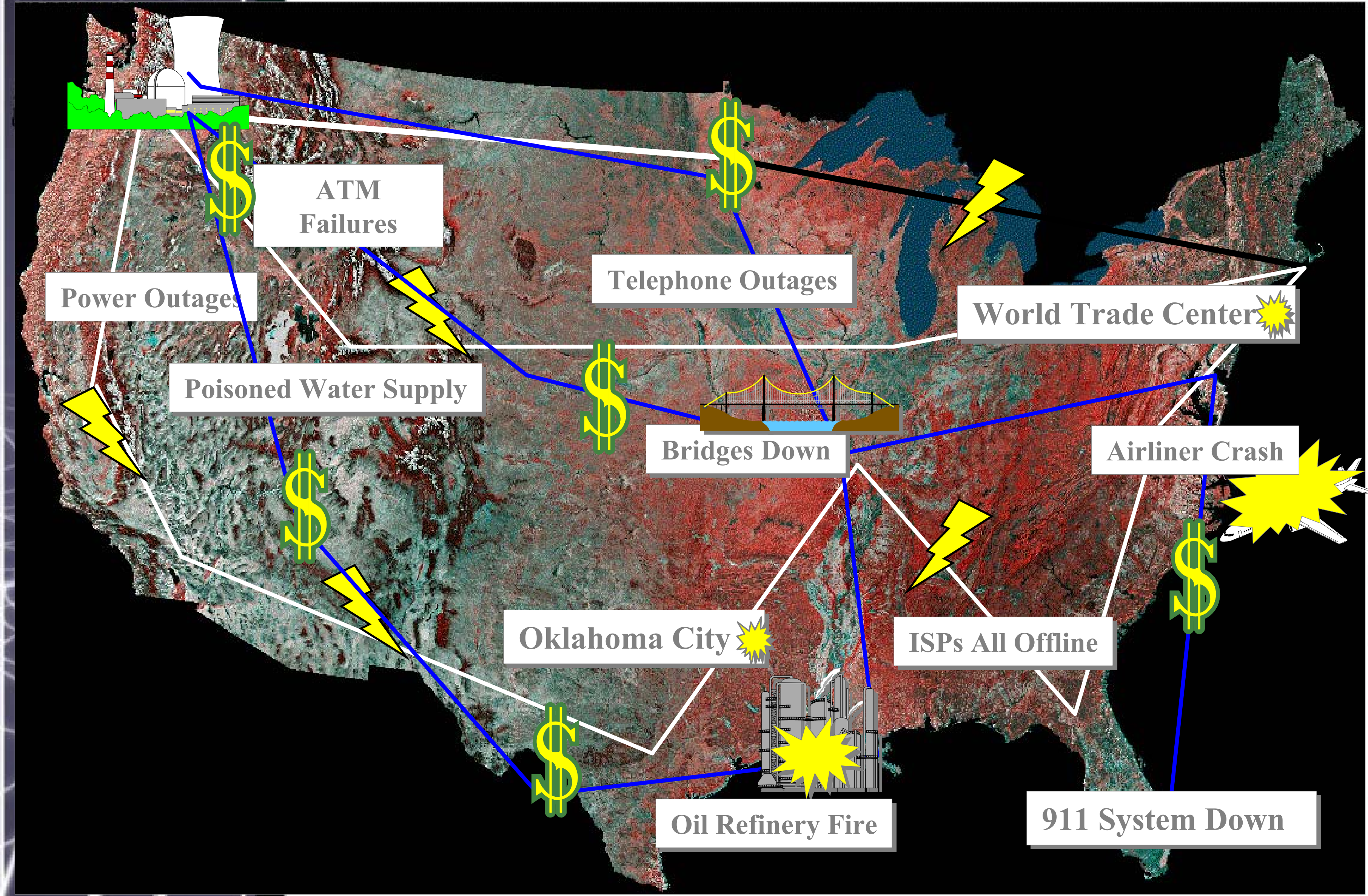
# Problem

- The term cyber terrorism actually minimizes the real issue
- Lots of activities going on in cyberspace
- We are at war – from many fronts

# Advantages

- Low costs
- Immediate and unexpected action
- A veil of anonymity
- Global reach
- Little risk
- Widely available and easy to use tools
- System interdependencies

# Imagine planning for these contingencies.



ATM Failures

Telephone Outages

Power Outages

World Trade Center

Poisoned Water Supply

Bridges Down

Airliner Crash

Oklahoma City

ISPs All Offline

Oil Refinery Fire

911 System Down

Unrelated events or strategic attack?

# Guided Weapon

**“The electron is the ultimate guided weapons system.”**

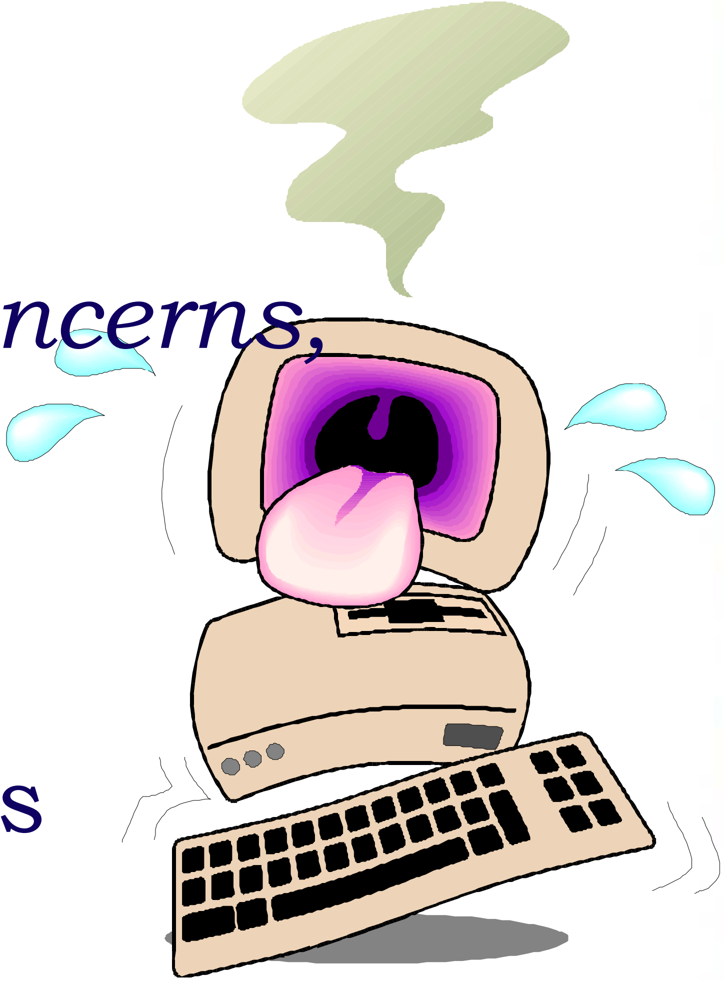
*--Dr. John Deutch,*

*Director, CIA*

*Testimony to U.S. Senate Permanent Subcommittee on Investigations Hearings, 25 June 96*

# Overview

- Introduction
- *Concepts, Concerns, Impacts*
- Case Studies
- Issues
- Contributions
- Conclusion



# Information Assurance

- **Protect** information and information systems from intentional, unintentional, and natural threats
- **Detect** threats to information and information systems
- **Restore** capabilities in an efficient and prioritized manner
- **Respond** appropriately with an integrated, coordinated, and focused effort to cope with, reduce, or eliminate the effects of attacks or intrusions

# Critical Infrastructures

"…the nation's critical infrastructures—telecommunications, water supply, electric power, banking and others—have substantial vulnerabilities that can be exploited by terrorists and foreign powers."

--*General Robert T. Marsh*
*Chairman, President's Commission on Critical Infrastructure Protection*

# Critical Infrastructures

"Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."

--*President William J. Clinton, Executive Order 13010*

# Critical Infrastructures

Government Operations

Gas & Oil Storage and Delivery

Emergency Services

Water Supply Systems

Telecommunications

Banking & Finance

Electrical Energy

Transportation

# Targetability

- The US is extremely targetable
- US contains 42% of the world’s computing power – 1997 figures
- Advanced societies increasingly dependent on vulnerable systems
- A **national** digital nervous system

# Sept 11th

- Cascading fallout
- Loss of telecommunications impacted financial transactions and electric power delivery
- Insurance rates increasing
  - Loss of $40 billion
  - Difficult to cover another large loss

# Sept 11th

- Ireland wants to sell minority stake in Aer Lingus
- Midway Airlines suspended flights Sept 12th in preparation for Chapter 11 filing

# Sept 11th

- Thousands of airline employees laid off
- Tourism industry
- Clothing industry
- Other industries in other countries

# Sept 11th

- Not helping an already sluggish economy
- Canada
  - Canadian dollar at record low
  - Plants shut down
  - Border delays hurt exports and tourism
  - Millions of jobs dependent upon our bilateral trade relationship

# Sept 11th

- US
  - Houses going unsold
  - Layoffs
  - Buy new car at 0%
  - Analysts indicate USPS reeling
  - Boeing layoffs: each lost Boeing employee = 1.7 employees in related industries
  - Tourism in the states

# Sept 11th

- Loss of friends and family
- People afraid world-wide
- “We’ve lost our innocence.”

# Critical Infrastructures

- Essential to economic and national security of US
- Vital to health, welfare, and safety
- Increasingly interdependent and interconnected systems

# Critical Infrastructures

- Owners & operators primary responsibility for protecting
- Generally not designed to cope with significant military or terrorist threats
- Government and industry must work together to deal with protecting our homeland

# Critical Infrastructures

- Requires an unprecedented partnership
- Goal - assured service delivery

# Information Warfare

- Nations working on capability
- In their war plans
- Stress the power of IW against civilian infrastructures - Tenet

# Information Warfare

*". . . attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence."*

*Sun Tzu, The Art of War*
*c. 350 B.C.*

# Information Warfare

"An adversary wishing to destroy the United States only has to mess up the computer systems of its banks by hi-tech means. This would disrupt and destroy the US economy."

China's People's Liberation Daily
February, 1996

# No Problem?

"To suppose that national utilities and infrastructure could be taken out by cyber terrorists, is, quite frankly, bollocks."

--Neil Barrett
Information Risk Management

# Omega Engineering

- Tim Lloyd planted a software time bomb
- Destroyed software controlling manufacturing machines
- $10 million + in losses
- $2 million + for reprogramming
- 80 layoffs

# California Dams

- Hacker named Infomaster
- Hacked into Bureau of Land Management’s Portland network
- Roamed BLM’s national network
- In Sacramento, obtained root access to computers controlling every dam in northern California

# Key Targets

- Culpepper Switch – handles all federal funds transfers & transactions
- Electronic Switching System – nationwide system that manages all telephone communications
- Time Distribution System – all major events depend on accurate time as recorded by government atomic clocks

# Overview

- Introduction
- Concepts, Concerns, Impacts
- *Case Studies*
- Issues
- Contributions
- Conclusion

# Case Studies

- FAA’s Air Traffic Control Systems
- Power Grid

# Air Traffic Control Systems

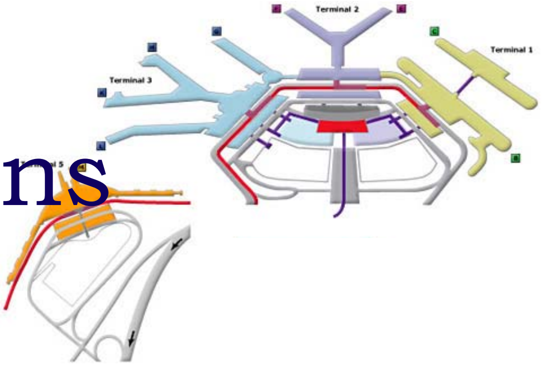
- ATC security has “serious and pervasive problems”
- Background checks
- Physical security
- Vulnerabilities
- Security program
- Intrusion detection
- Awareness training

# Air Traffic Control Systems

- I&A not always required
- External users not always authenticated
- Known vulnerabilities are not tracked
- Unauthorized hardware & software
- Inconsistent anti-virus
- Other vulnerabilities identified as being too sensitive to include

# Air Traffic Control Systems

- Interconnectedness
- Increasing reliance on commercially available HW/SW
- Only 6 of 90 systems accredited
- Contingency plans inadequate

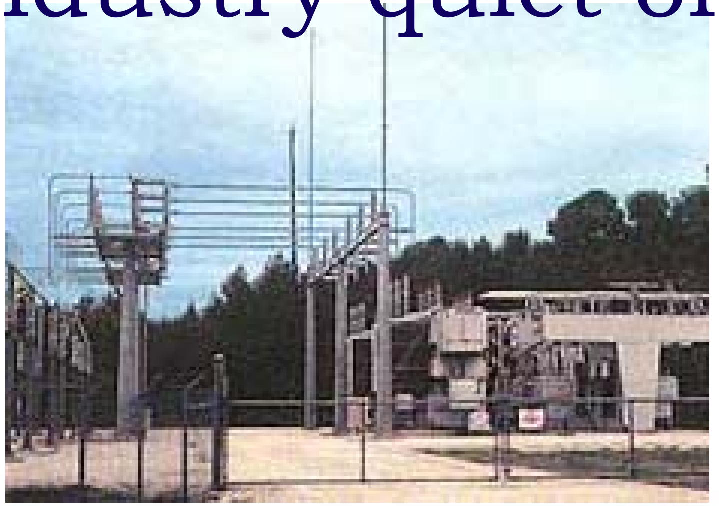


# Air Traffic Control Systems

- Massachusetts
- Teen broke into Bell Atlantic system
- Disabled communications with the Worcester airport
- Control tower couldn’t turn on runway lights
- No intent – what if he was malicious?

# Power Grid

- Actual incidents hard to find
- ELIGIBLE RECEIVER
- Electric industry quiet on the issue



# Power Grid

Information from an Electric Power Information Assurance Risk Assessment, conducted by The President’s National Security Telecommunications Advisory Committee’s Information Assurance Task Force

# Power Grid

- No standard control center configuration
- Interfaces to:
  - Corporate information systems
  - Other utilities or power pools
  - Supporting vendors
  - Remote maintenance/administration ports

# Power Grid

- Intrusion reported by one electric utility
  - Access to nuclear engineering support network
  - Accessed databases, altered logs
- Maintenance dial-in passwords not changed

# Power Grid

- Substations becoming more and more automated – an intruder could reset breaker tolerance levels
- Much of the control communications traffic is carried on public networks
- Deregulation – a wholesale market for power generation

# Power Grid

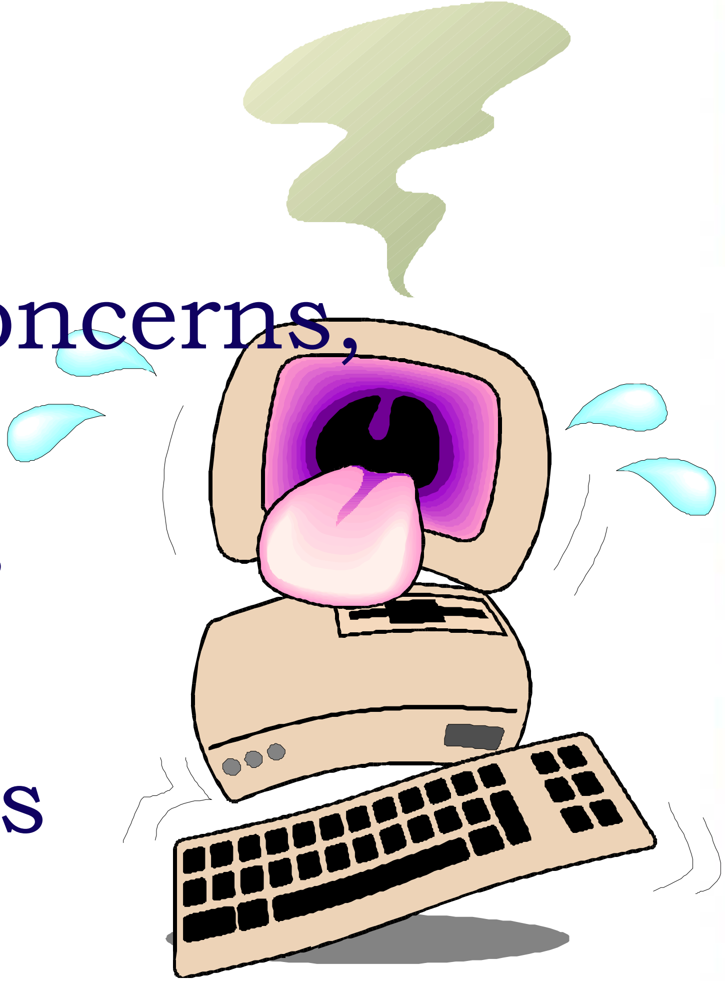
- Sale of bulk power over great distances
- Ever more dependence on cyber systems
- An increasing focus on E-commerce

# Power Grid

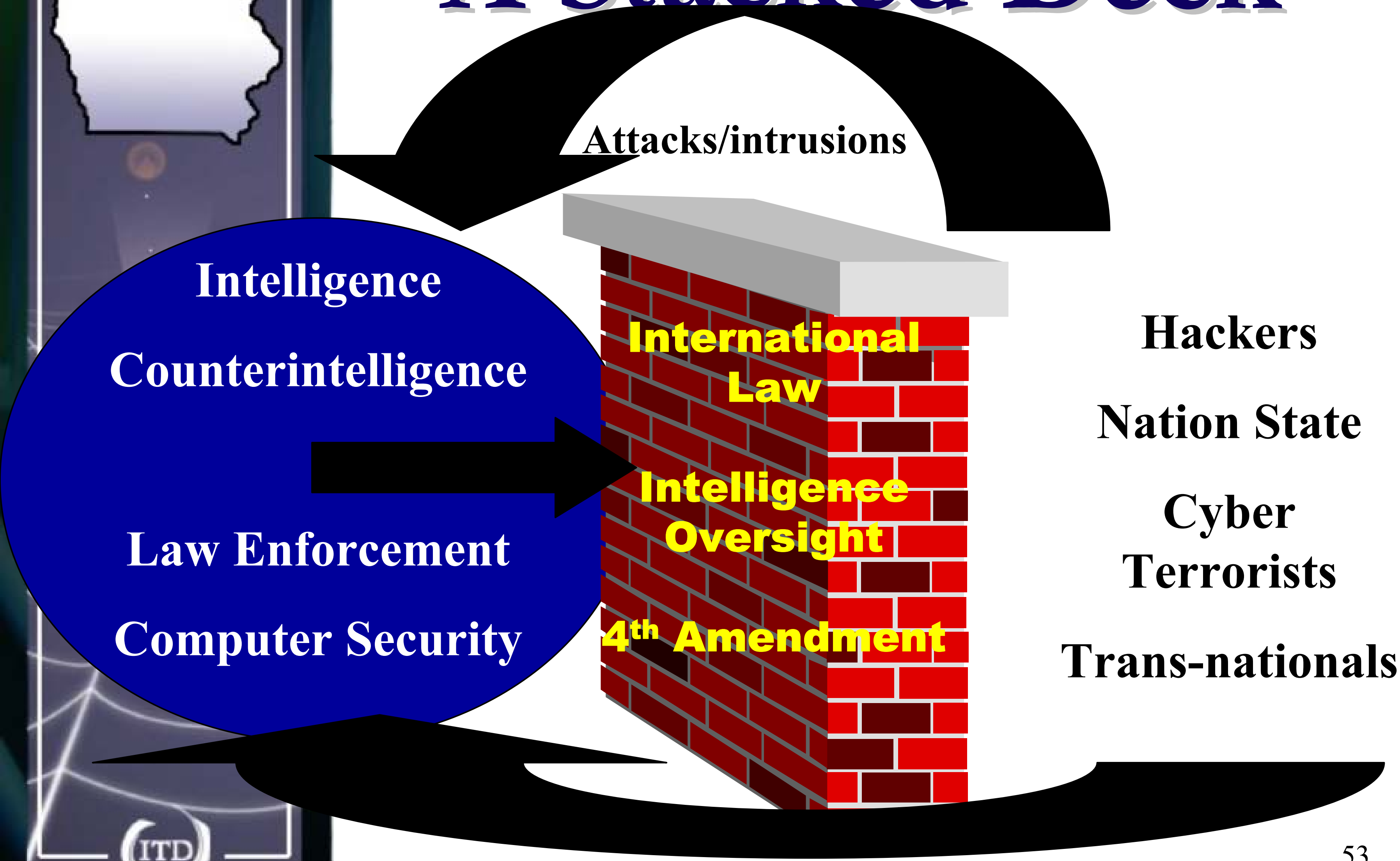
- Looking at implementing further controls
- Security investments hard to sell to senior managers
- Physical destruction determined to be a much greater risk

# Overview

- Introduction
- Concepts, Concerns, Impacts
- Case Studies
- *Issues*
- Contributions
- Conclusion



# A Stacked Deck



Attacks/intrusions

Intelligence

Counterintelligence

Law Enforcement

Computer Security

International Law

Intelligence Oversight

4th Amendment

Hackers

Nation State

Cyber Terrorists

Trans-nationals

# Most Breaches Unreported

- Don’t know they’ve been attacked
- Don’t want their image tarnished
- Makes it difficult to defend
- Difficult to catch and prosecute
- 21st Century crimes, 18th Century laws

# Issues

- Full range of the threat is unknown
- Lack of appropriate personnel
- Who is the perpetrator?
- Where is the perpetrator?
- What is the impact?
- Who should respond, and in what manner?
- What is an act of terrorism? An act of war? A hack? An accident?

# Issues

- Huge interdependencies – that we don’t understand
- No leadership from the top – uncoordinated effort
- Focus on productivity and functionality versus security in system software
- Private entities not held responsible
- Fighting a different enemy – networked organizations

# Issues

- Suspicion and distrust of government
- Inadequate intelligence gathering
- State liaison non-existent

# Facts

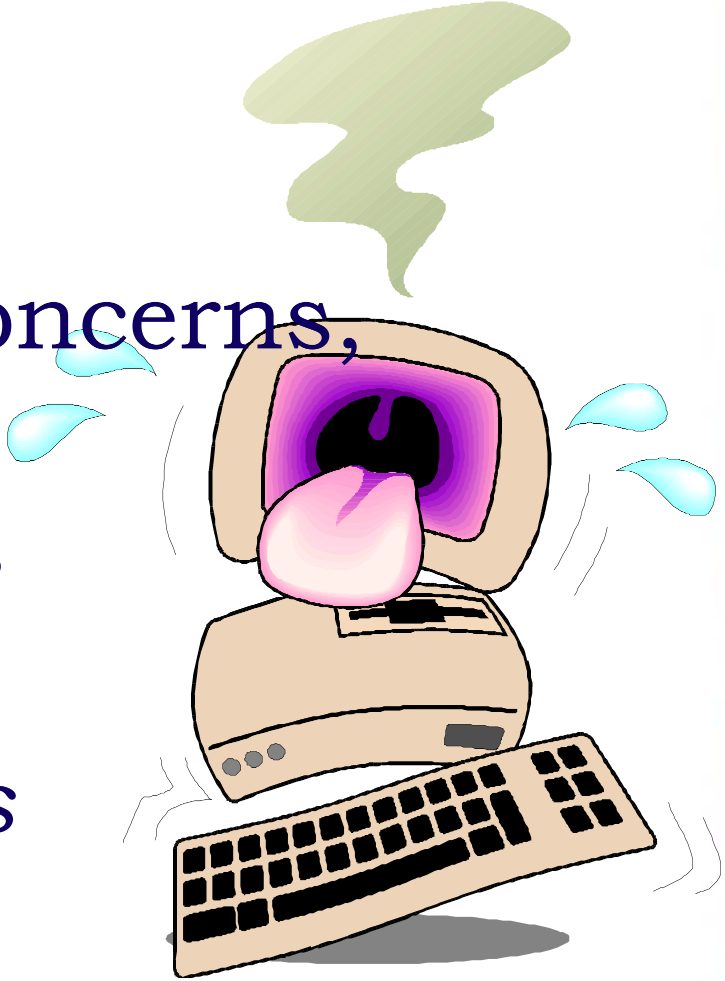
- The adversary is competent
- We won’t know who they are
- We won’t know their location
- We won’t know it’s coming
- No boundaries

# Rome Labs, 1994

- 2 hackers
- 26 days of attacks
- Over 150 intrusions from 10 different points of origin
- At least 8 countries used as a conduit

# Overview

- Introduction
- Concepts, Concerns, Impacts
- Case Studies
- Issues
- *Contributions*
- Conclusion



# Recommendations

- Raise national awareness – all stakeholders
- Infrastructures must work together
- Develop a national strategy
- Establish requirements

# Recommendations

- Shift focus from functionality and mainstream users to inherently secure systems
- Focus on information assurance, not just information protection
- Enterprise approach
- Be prepared!

# Recommendations

- Treat state and local governments as a sector
- Legislate as necessary
- Fund
- Train
- Enhance intelligence

# Recommendations

- Partner with DoD
  - Training
  - Troops to industry
  - Research and development
  - Contracts
  - CNA
- Use information operations fundamentals

# Recommendations

- Defensive information operations
  - Info assurance
  - OPSEC
  - Physical security
  - Counterdeception
  - Counter-propaganda
  - Counterintelligence
  - Public affairs

# Recommendations

- Offensive IO
  - OPSEC
  - Deception
  - Psychological operations
  - Electronic warfare
  - Computer network attack

# NIPC

- FBI’s National Infrastructure Protection Center
- Created in response to PDD 63
- National critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation & response entity
- The local level’s link to federal efforts

# NIPC

- Share, analyze, and disseminate information
- Training for federal, state, and local cyber investigators
- Coordinate FBI computer intrusion investigations

# InfraGard

- Part of the NIPC
- Outreach and information sharing with public and private sector
- Owners & operators of critical infrastructures
- Local chapters
- An Iowa chapter now in operation

# InfraGard

- Formal and informal information exchange
- Promotes protection of critical infrastructures
- Representatives from private industry, government agencies, academic institutions, state & local law enforcement

# InfraGard

- Intrusion alert network
- Secure Web site
- Seminars and training
- Meetings with colleagues
- Develop contacts with each other and local FBI personnel

# FBI Benefits

- More reported intrusions
- Satisfies PDD 63
- New channels for threat warning dissemination
- New contacts in business community

# Private Sector Benefits

INFRAGARD
PARTNERSHIP FOR PROTECTION

- Threat warnings
- Better understanding of law enforcement and available resources
- Education and training
- Interaction with a wide variety of personnel

# NIPC's IAW Program

- Indications, Analysis, and Warning Program: Electric Power
- Information sharing between the power industry and the NIPC
- Coordinate through the power system control centers (24x7x365)
- Report incidents up to NIPC
- NIPC reports warnings downward

# The CIAO

- The Critical Infrastructure Assurance Office
- Created by PDD 63
- Mission
  - Develop a national plan
  - Coordinate departmental analyses
  - Coordinate national education & awareness program
  - Coordinate legislation & public affairs

# PCIS

- Partnership for Critical Infrastructure Security
- Supposed to coordinate cross-sector initiatives
- Industry driven
- Setting up information sharing and analysis centers

# Homeland Security

- Office of Homeland Security, Tom Ridge
- Cyberspace security – Richard Clarke

# Iowa

- EMD's Interagency Domestic Preparedness Working Group
- ITD taking the lead w/EMD support – Critical Infrastructure Assurance Coordinator
- Held conference on 25 April, STARC Armory
- Beginning to identify issues and start the planning process
- InfraGard chapter

# Iowa

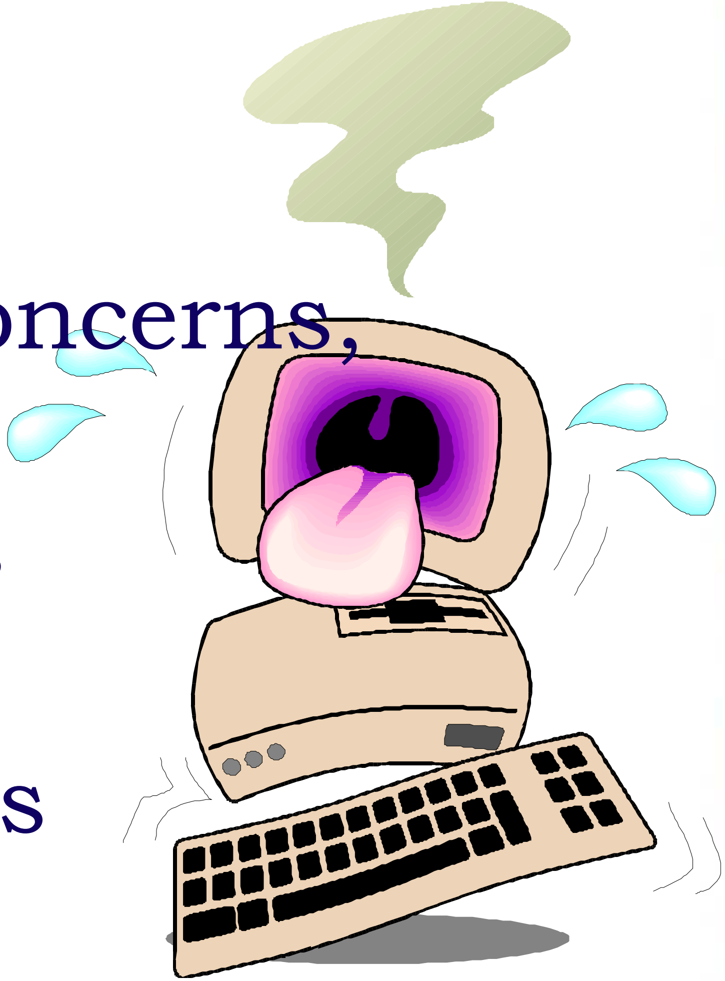
- Homeland Security Advisor – Ellen Gordon
- Cyber piece is included in the effort
- Critical target prevention planning

# Iowa

- Elevate the issues
- Identify appropriate personnel
- Share information and present a common approach
- Develop policies and standards
- Obtain necessary training
- Exercise
- Identify interdependencies

# Overview

- Introduction
- Concepts, Concerns, Impacts
- Case Studies
- Issues
- Contributions
- *Conclusion*



# Conclusion

- The threat is real and becoming more apparent
- As our capabilities increase, so does our risk
- Must address the issue in some way
- Not a lot of coordinated action up to now